Diversity-Multiplexing Tradeoff for the Multiple-Antenna Wire-tap Channel

Melda Yuksel, *Member, IEEE*, and Elza Erkip, *Senior Member, IEEE*

Abstract

In this paper the fading multiple antenna (MIMO) wire-tap channel is investigated under short term power constraints. The *secret* diversity gain and the *secret* multiplexing gain are defined. Using these definitions, the *secret* diversity-multiplexing tradeoff (DMT) is calculated analytically for no transmitter side channel state information (CSI) and for full CSI. When there is no CSI at the transmitter, under the assumption of Gaussian codebooks, it is shown that the eavesdropper *steals* degrees of freedom from the source-destination channel, and the secret DMT depends on the remaining degrees of freedom. When CSI is available at the transmitter (CSIT), the eavesdropper *steals* transmitter antennas, but not the degrees of freedom of the source-destination channel. This dependence on the availability of CSI is unlike the DMT results without secrecy constraints, where the DMT remains the same for no CSI and full CSI at the transmitter under short term power constraints. A *zero-forcing* type scheme is shown to achieve the secret DMT when CSIT is available.

Keywords: Diversity-multiplexing tradeoff, MIMO, secrecy, wire-tap channel.

I. Introduction

In wireless communications, messages are transmitted publicly. Any transmission can be overheard by nearby nodes. If illegitimate, passive listeners trying to understand messages, known as eavesdroppers, are present in the environment, then all confidential information such as user IDs, passwords, or credit card numbers become vulnerable and can be identified. In addition to voice, image, video, and data transmissions, future applications envision wireless transmission of sensitive information such as personal and locality information. Therefore, wireless security is an essential system requirement.

The material in this paper was presented in part at the 42nd Annual Conference on Information Sciences and Systems, CISS 2008, Princeton, NJ.

M. Yuksel with the Electrical and Electronics Engineering Department, TOBB University of Economics and Technology, Ankara, Turkey (e-mail: yuksel@etu.edu.tr).

E. Erkip is with the Electrical and Computer Engineering Department, Polytechnic Institute of New York University, Brooklyn, NY 11201 USA (e-mail: elza@poly.edu).

In current wireless systems, protection against eavesdropping is provided at higher layers of the Open Systems Interconnection (OSI) reference model. Transport, network or application layer protocols aim to prevent eavesdropping using encryption. However, cryptographic algorithms are highly complex and are not robust. Thus, enhancing the current encryption techniques with unconditional security protocols, which cannot be broken even with infinite computing power, are of utmost importance for future development of wireless applications.

Physical layer security techniques provide unconditional secrecy through channel coding and complement higher layer security methods. Information-theoretic security investigates the fundamental limits of secure communication at the physical layer. One of the building blocks of information-theoretic security is the wire-tap channel. The physically degraded wire-tap channel was introduced in [1] and the fundamental coding structure to obtain perfect secrecy was established. Later in [2], these results were extended to less noisy and more capable broadcast channels. The secrecy capacity for the Gaussian wire-tap channel was found in [3]. Recently fading wire-tap channels are investigated in [4], [5], for which the ergodic secrecy capacity is calculated when both the transmitter and the receivers have channel state information (CSI). In [4] the ergodic secrecy capacity, when the source node does not have the eavesdropper's CSI, is also evaluated.

In wireless channels, multiple antennas increase robustness against fading, and also transmission rates. Multiple antennas are considered in the context of wire-tap channels in [6], [7]-[12]. In [7] the authors find the secrecy capacity of the Gaussian multiple-input multiple-output (MIMO) wire-tap channel, when the source and the destination have two antennas each and the eavesdropper has only a single antenna. Concurrent work in [8], [9] and [10] establish the secrecy capacity for the fading MIMO wire-tap channel under the full CSI assumption for arbitrary antenna numbers.

Although the ergodic behavior of fading channels is very important, when there are stringent delay constraints, ergodic capacity is not realizable. In this case, the outage formulation proves to be useful. For the wire-tap channel, outage approach was first considered in [6] and [13]. Outage probability for a target secrecy rate is also investigated in [5], when the source, the destination and the eavesdropper have CSI, and optimal power allocation policies that minimize the outage probability are calculated.

An important performance measure for MIMO fading channels that simultaneously considers probability of error and data rates is the diversity-multiplexing tradeoff (DMT), established in [14]. The DMT is a high SNR analysis and describes the fundamental tradeoff between the diversity gain and the multiplexing

gain. The diversity gain is the decay rate of the probability of error, and the multiplexing gain is the rate of increase of the transmission rate in the limit of high SNR. The DMT is strongly related to the probability of outage as probability of error is generally dominated by the outage event at high SNR.

In this paper we investigate the multiple-antenna wire-tap channel from the DMT perspective. We define the *secret* multiplexing gain, the *secret* diversity gain and the *secret* DMT. We argue that the eavesdropper can be thought of as "stealing" degrees of freedom from the source-destination channel, and the *secret* DMT depends on the remaining degrees of freedom, when there is no CSIT. This behavior is also observed in [15], [16] for compound channels only for the maximum multiplexing gain point. Our work can be thought of as a generalization of [15], [16], capturing the behavior for all diversity gains. We also argue that the secret DMT depends on the available CSI at the transmitter (CSIT). This is unlike the regular point-to-point DMT without security constraints, which is not affected from the transmitter CSI for constant-rate transmission. Under CSIT assumptions, we also suggest a *zero-forcing* type scheme, which achieves the secret DMT upper bounds.

Next, we introduce the system model in Section II and then state the secret DMT for no CSIT in Section III. Section IV covers the secret DMT when there is CSIT. We conclude in Section V.

II. System Model and Preliminaries

We consider a multiple-antenna wire-tap channel, in which the source, the destination and the eavesdropper have m, n and k antennas respectively. Both the destination and the eavesdropper have CSI about their incoming channels. In Section III we assume the source node does not have any transmit CSI. We will consider the case when the source has transmitter CSI in Section IV.

For each channel use the channel is represented as follows:

$$\mathbf{Y}_D = \mathbf{H}_D\mathbf{X} + \mathbf{Z}_D \tag{1}$$

$$\mathbf{Y}_E = \mathbf{H}_E\mathbf{X} + \mathbf{Z}_E. \tag{2}$$

In the above equations $\mathbf{X}$ is an $m \times 1$ vector, which denotes the transmitted source signal. $\mathbf{Y}_D$ and $\mathbf{Y}_E$ are $n \times 1$ and $k \times 1$ vectors, and represent the received signals at the destination and the eavesdropper respectively. Similarly, $\mathbf{Z}_D$ and $\mathbf{Z}_E$ are $n \times 1$, and $k \times 1$ vectors that indicate the independent additive noise at the destination and the eavesdropper. Both $\mathbf{Z}_D$ and $\mathbf{Z}_E$ have independent and identically distributed (i.i.d.) complex Gaussian entries with zero mean and variance 1. The matrices $\mathbf{H}_D$ and $\mathbf{H}_E$, consisting

of i.i.d. complex Gaussian entries with zero mean and unit variance, are of size $n \times m$, and $k \times m$. They respectively denote the channel gains between the source and the destination and the source and the eavesdropper.

When there is no secrecy constraint, the source fixes its transmission rate at $R^{(T)}$ and aims to transmit the message W, $W \in \mathcal{W} = \{1, 2, ..., 2^{NR^{(T)}}\}$, in N channel uses. The destination declares an error if its decision $\hat{W} \neq W$, $\hat{W} \in \mathcal{W}$. This probability is shown to be dominated by the outage event, whose probability is given by

$$P_e(\mathrm{SNR}) \doteq P(R < R^{(T)})^1,$$

where $R = I(\mathbf{X}; \mathbf{Y}_D)$ is the instantaneous mutual information corresponding to the chosen transmission scheme. The diversity and multiplexing gains, d and r, are respectively defined in [14] as

$$\lim_{\mathrm{SNR}\to\infty} \frac{\log P_e(\mathrm{SNR})}{\log \mathrm{SNR}} = -d,$$

and

$$\lim_{\mathrm{SNR}\to\infty} \frac{R^{(T)}(\mathrm{SNR})}{\log \mathrm{SNR}} = r.$$

The optimum diversity-multiplexing tradeoff $d(r)$ is the piecewise linear function joining the points

$$d_{m,n}(l) = (m - l)(n - l),$$

$l = 0, 1, ..., \min\{m, n\}$. The degrees of freedom in this system is $\min\{m, n\}$, and the multiplexing gain r can increase up to this value. Each additional multiplexing gain costs the system a single degree of freedom, and the diversity gain decreases as the multiplexing gain increases.

Under secrecy constraints, the rate-equivocation rate region [1] indicates the transmission rates over the main channel and the level of obscurity at the eavesdropper. A rate–equivocation rate pair (R, R_s) is achievable if there exists a sequence of $(2^{NR}, N)$ codes with $P(\hat{W} \neq W) \to 0$, as $N \to \infty$ and

$$\lim_{N\to\infty} \frac{1}{N} H(W|Y_E^N) \geq R_s.$$

The equivocation rate R_s describes the eavesdropper's confusion about the message W given its observation Y_E^N. An operating point in the rate-equivocation rate region is called *perfectly secure*, if the

[1]The expression $f_1(\mathrm{SNR}) \doteq f_2(\mathrm{SNR})$ is used to mean $\lim_{\mathrm{SNR}\to\infty} \log f_1(\mathrm{SNR})/\log \mathrm{SNR} = \lim_{\mathrm{SNR}\to\infty} \log f_2(\mathrm{SNR})/\log \mathrm{SNR}$. In the rest of the paper, inequalities are also defined similarly.

equivocation rate R_s is arbitrarily close to the information rate R. Moreover, the perfect secrecy rate

$$R_s = [I(\mathbf{X};\mathbf{Y}_D) - I(\mathbf{X};\mathbf{Y}_E)]^+ \tag{3}$$

is achievable [2] for any input distribution $p(\mathbf{X})$, where x^+ denotes $\max\{0, x\}$. The capacity-equivocation rate region, $\mathcal{C}$, is the closure of the set of all achievable rate-equivocation pairs (R, R_s). The highest perfectly secure rate is called the secrecy capacity [1].

To briefly describe how we achieve the perfect secrecy rate in (3) for some input distribution $p(\mathbf{X})$, we define $A = 2^{NR_s}$, $B = 2^{NI(\mathbf{X};\mathbf{Y}_E)}$ and the sets $\mathcal{A} = \{1, ..., A\}$ and $\mathcal{B} = \{1, ..., B\}$. The source forms $AB = 2^{NI(\mathbf{X};\mathbf{Y}_D)}$ channel codewords $\mathbf{X}^N$ i.i.d. with $p(\mathbf{X})$. In order to send a secret message $a \in \mathcal{A}$, the source chooses b uniformly from the set $\mathcal{B}$, forms $w = (a, b)$ and maps w into a channel codeword $\mathbf{X}^N$. In other words for each secret message a, the source randomly chooses from one of the B dummy codewords to confuse the eavesdropper. As the total number of codewords in the source code book is equal to $2^{NI(\mathbf{X};\mathbf{Y}_D)}$, the destination can reliably decode w and hence a. However, the eavesdropper can only decode the index b and has no information about the secret message a. Thus perfect secrecy can be achieved.

In this work, we assume perfect secrecy, $R = R_s$, and investigate the high SNR behavior of the secrecy probability of error with a target secrecy rate equal to $R_s^{(T)}(\mathrm{SNR})$. We assume the system is delay-limited and requires constant secrecy rate transmission. There is also short-term average power constraint $m\mathrm{SNR}$ that the transmitter has to satisfy for each codeword transmitted. We define the *secret* multiplexing gain as

$$\lim_{\mathrm{SNR}\to\infty} \frac{R_s^{(T)}(\mathrm{SNR})}{\log \mathrm{SNR}} \triangleq r_s.$$

The secret multiplexing gain r_s shows how fast the target secrecy rate scales with increasing SNR. The *secret* diversity gain, d_s, is equal to

$$\lim_{\mathrm{SNR}\to\infty} \frac{\log P_e(\mathrm{SNR})}{\log \mathrm{SNR}} \triangleq -d_s,$$

where $P_e(\mathrm{SNR})$ denotes the probability of error under secrecy constraints. In this paper, we establish the tradeoff between secret diversity gain d_s and the secret multiplexing gain r_s, $d_s(r_s)$.

In a system with secrecy constraints, the probability of error is due to two events: Either the destination does not receive the secret message reliably, or perfect secrecy is not achieved [17]. When the channel block

length-N is long enough and good codes are used, probability of error is dominated by the corresponding outage events. Then we can write

$$\begin{aligned} P_e(\mathrm{SNR}) &\doteq P(\text{outage}) \\ &= P(\text{perfect secrecy outage or main channel outage}) \\ &\leq P(\text{perfect secrecy outage}) + P(\text{main channel outage}). \end{aligned} \tag{4}$$

On the other hand,

$$P_e(\mathrm{SNR}) \geq P(\text{perfect secrecy outage}). \tag{5}$$

In the following we will use these upper and lower bounds on probability of error to establish the secret DMT.

Finally, note that we assume a single transmission block of N channel uses under short-term power constraint. This is unlike the scenario in [18], where there are many blocks to communicate and a long-term power constraint. In [18] the first communication block is merely used to generate a secret key, and in the next block this key is used to enhance secrecy, while another key is generated to be used in the following block. In our system, communication session lasts a single code block, during which secrecy has to be maintained. In other words, the transmitter and the receiver have to start secure communication immediately at the beginning of the transmission block.

III. No Channel State Information at the Source

When there is no CSIT the MIMO wire-tap channel capacity is not known. However, motivated by the fact that when all nodes in the system have CSI, Gaussian codebooks are optimum, [8], [9], [10], we assume Gaussian codebooks. We also conjecture that sending independent signals at equal power at each antenna is optimal at high SNR, as all the entries of $\mathbf{H}_D$ and $\mathbf{H}_E$ respectively are identically distributed. As the source node does not have CSI, it has no preference over one *direction* over the other. Under these assumptions the input covariance matrix Q is a diagonal matrix $Q = \mathrm{SNR}\mathbf{I}_m$, where $\mathbf{I}_m$ indicates

an identity matrix of size m. Then, we can write the achievable perfect secrecy rate in (3) as

$$\begin{aligned} R_s &= \left[\log\left|\mathbf{I}_n + \mathbf{H}_D Q \mathbf{H}_D^\dagger\right| - \log\left|\mathbf{I}_k + \mathbf{H}_E Q \mathbf{H}_E^\dagger\right|\right]^+ \\ &= \left[\log \frac{\prod_{i=1}^{L}(1+\lambda_i \mathrm{SNR})}{\prod_{i=1}^{k}(1+\mu_i \mathrm{SNR})}\right]^+, \end{aligned} \tag{6}$$

where $L = \min\{m, n\}$, $0 \leq \lambda_1 \leq ... \leq \lambda_L$ are the ordered eigenvalues of the matrix $\mathbf{H}_D \mathbf{H}_D^\dagger$, $0 \leq \mu_1 \leq ... \leq \mu_k$ are the ordered eigenvalues of the matrix $\mathbf{H}_E \mathbf{H}_E^\dagger$, and $\dagger$ denotes the conjugate transpose.

Theorem 1: For the multiple-antenna wire-tap channel defined in (1) and (2), with full CSI at the destination and the eavesdropper about their incoming channel gains and no CSI at the source, if $k < \min\{m, n\}$, the secret diversity-multiplexing tradeoff achieved by isotropic Gaussian codebook is a piece-wise linear function joining the points $(l, d_s(l))$, where $l = 0, 1, ..., \min\{m, n\} - k$ and

$$d_s(l) = (m - k - l)(n - k - l).$$

If $k \geq \min\{m, n\}$, then the secret diversity-multiplexing tradeoff reduces to the single point $(0, 0)$.

Proof: To find the secret DMT we first find a lower bound and an upper bound on the probability of the secrecy rate outage; $P(\text{perfect secrecy outage}) = P(R_s < R_s^{(T)})$, where $R_s^{(T)} = r_s \log \mathrm{SNR}$, and show that both of these bounds have the same DMT $d_{m-k,n-k}(r_s)$. The details of these bounds are presented in Appendix I.

To attain perfect secrecy the source transmits at rate $R^{(T)} = R_s^{(T)} + \min\{m, k\} \log \mathrm{SNR} = (r_s + \min\{m, k\}) \log \mathrm{SNR}$ bits/channel use, where the target secret communication rate is $R_s^{(T)}$ bits/channel use. Following the secrecy achievability scheme in [2], also outlined in Section II, the total number of codewords in the channel codebook is equal to $2^{NR^{(T)}}$, and the number of dummy codewords used for each secret message is fixed and equal to $B = 2^{N \min\{m,k\} \log \mathrm{SNR}}$. Then the main channel is in outage when the destination cannot decode rate $R^{(T)}$, which has the probability

$$P(\text{main channel outage}) = P\left(I(\mathbf{X}; \mathbf{Y}_D) < R^{(T)}\right) \tag{7}$$

$$= P\left(I(\mathbf{X}; \mathbf{Y}_D) < (r_s + \min\{m, k\}) \log \mathrm{SNR}\right) \tag{8}$$

$$\stackrel{(a)}{\doteq} \mathrm{SNR}^{-d_{m,n}(r_s + \min\{m,k\})} \tag{9}$$

$$= \begin{cases} \mathrm{SNR}^{-d_{m-k,n-k}(r_s)} & \text{if} \quad k < m \\ 0 & \text{if} \quad k \geq m \end{cases}, \tag{10}$$

where (a) is due to [14].

Overall, if $k < m$ the upper bound on the probability of error (4) becomes equal to

$$\begin{aligned} P_e(\mathrm{SNR}) &\doteq \mathrm{SNR}^{-d_{m-k,n-k}(r_s)} + \mathrm{SNR}^{-d_{m-k,n-k}(r_s)} \\ &\doteq \mathrm{SNR}^{-d_{m-k,n-k}(r_s)}. \end{aligned}$$

As the lower bound on probability of error (5) is the same, we conclude that the secret DMT is equal to $d_{m-k,n-k}(r_s)$ if $k < m$. If $k \geq m$, the secret DMT is the single point $(0, 0)$. ■

Theorem 1 states that the eavesdropper costs the system $\min\{m, k\}$ degrees of freedom, which affects the whole secret DMT curve. When the degrees of freedom in the source-eavesdropper channel, $\min\{m, k\}$, is equal to k, then the secret system becomes equivalent to an $(m-k) \times (n-k)$ system. However, if $\min\{m, k\} = m$, then no degrees of freedom are left for the main channel, as $m \geq \min\{m, n\}$, and the secret DMT reduces to the single point $(0, 0)$.

Fig.1 shows an example secret DMT when there is no CSIT for the wire-tap channel, when the source, the destination and the eavesdropper have 3, 4, and 2 antennas respectively; $m = 3$, $n = 4$ and $k = 2$. We observe that for the *secret* channel only one degree of freedom is left, and the maximum *secret* diversity can be 2. The figure also compares the secret DMT to the 3×4 channel DMT without secrecy constraints. We can observe the effect of secrecy constraints not only on the degrees of freedom, but also on diversity, for all possible secret multiplexing gain values.

IV. Channel State Information at the Source

In the previous section secret DMT is established for MIMO wire-tap channels without CSIT. In this section we assume that transmitter has perfect CSI about the channel between itself and the eavesdropper, as well as its channel to the destination. While it may be possible for the source to obtain eavesdropper CSI if both the destination and the eavesdropper are part of the same network, the full CSIT assumption may be harder to justify if the eavesdropper is merely an illegitimate listener. Nevertheless, this assumption will help us understand the limitations and properties of secret DMT. Note that secret DMT is still a meaningful metric as we consider constant secret rate applications that operate under short-term power constraints, which can suffer from outage despite the available CSIT.

In the next subsection we establish the secret DMT with CSIT and in Section IV-B we investigate different schemes that achieve the best secret DMT with CSIT.

A. Secret DMT with CSIT

The secrecy capacity for the non-fading MIMO wire-tap channel with channel knowledge both at the receivers (the destination and the eavesdropper) and the transmitter (the source) is found in [8], [9], [10] as

$$C_s = \max_{\substack{Q \succeq 0, \\ \mathrm{Tr}(Q) \leq m\mathrm{SNR}}} \log \left| \mathbf{I}_n + \mathbf{H}_D Q \mathbf{H}_D^{\dagger} \right| - \log \left| \mathbf{I}_k + \mathbf{H}_E Q \mathbf{H}_E^{\dagger} \right|. \tag{11}$$

To establish the secret DMT with CSIT, we first need the following lemma.

Lemma 1: If $k < \min\{m, n\}$, then $p = \dim\{\mathrm{Null}(\mathbf{H}_\mathrm{D})^{\perp} \cap \mathrm{Null}(\mathbf{H}_\mathrm{E})\} > 0$, where $\mathrm{Null}(\mathbf{H}_D)^{\perp}$ is the orthogonal complement of the null space of $\mathbf{H}_D$ and $\mathrm{Null}(\mathbf{H}_E)$ is the null space of $\mathbf{H}_E$. If $n \leq k < m$ or $k \geq m$, then $p = 0$.

Proof: The subspaces $\mathrm{Null}(\mathbf{H}_E)$ and $\mathrm{Null}(\mathbf{H}_D)^{\perp}$ are defined in the vector space $\Re^m$. If $k < \min\{m, n\}$, then $\mathrm{Null}(\mathbf{H}_E)$ and $\mathrm{Null}(\mathbf{H}_D)^{\perp}$ respectively have dimensions $m - k$ and $q = \min\{m, n\}$, and have the basis sets $\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_{m-k}\}$ and $\mathcal{W} = \{\mathbf{w}_1, \mathbf{w}_2, ..., \mathbf{w}_q\}$. In other words, the sets $\mathcal{U}$ and $\mathcal{W}$ are both linearly independent sets. However, as $m - k + q > m$, $\mathcal{U} \cup \mathcal{W}$ is linearly dependent. The intersection of the hyper-planes $\mathcal{U}$ span and $\mathcal{W}$ span, includes at least one non-zero vector. Thus $p > 0$.

If $n \leq k < m$, then the basis sets $\mathcal{U}$ and $\mathcal{W}$ are same as above with $q = n$. However, in this case $\mathcal{U} \cup \mathcal{W}$ is a linearly independent set, as $m - k + q = m - k + n \leq m$. The intersection of the hyper-planes $\mathcal{U}$ span and $\mathcal{W}$ span only include $\{\mathbf{0}\}$ and thus $p = 0$.

If $k \geq m$, then Null$\mathbf{H}_E$ consists of only $\{\mathbf{0}\}$. Then $\mathrm{Null}(\mathbf{H}_D)^{\perp} \cap \mathrm{Null}(\mathbf{H}_E) = \{\mathbf{0}\}$, and thus $p = 0$. ■

Theorem 2: For the multiple-antenna wire-tap channel defined in (1) and (2), with full CSI at all the terminals, if $k < m$, the secret diversity-multiplexing tradeoff, $\hat{d}_s(r_s)$ is a piecewise linear function joining the points $(l, \hat{d}_s(l))$, where $l = 0, 1, ..., m - k$ and

$$\hat{d}_s(l) = (m - k - l)(n - l).$$

If $k \geq m$, then the secret diversity-multiplexing tradeoff reduces to the single point $(0, 0)$.

Proof: When the secrecy capacity is expressed as in (11), it is hard to calculate the secret DMT. We make use of the high SNR secrecy capacity approximations provided in [19], [9] to find the secret DMT. We investigate the three cases $k < \min\{m, n\}$, $n \leq k < m$, and $k \geq m$ separately.

For the first case $k < \min\{m, n\}$, $p > 0$ by Lemma 1 and $\mathbf{H}_E$ is not full column rank; i.e. $k < m$,

then the secrecy capacity at high SNR is given by [19], [9]

$$\tilde{C}_s(\mathrm{SNR}) = \sum_{j:\sigma_j \geq 1} \log \sigma_j^2 + \log \left| \mathbf{I}_n + \frac{m\mathrm{SNR}}{p} \mathbf{H}_D \mathbf{H}_E^{\perp} \mathbf{H}_D^{\dagger} \right| + o(1), \tag{12}$$

where $o(1) \to 0$ when $\mathrm{SNR} \to \infty$, $\mathbf{H}_E^{\perp} \in \mathbb{C}^{m \times m}$ is the projection matrix onto $\mathrm{Null}(\mathbf{H}_E)$, and σ_j, $j = 1, ..., \min\{m, n\} - p$, are the generalized singular values of matrices $\mathbf{H}_D$ and $\mathbf{H}_E$. To find the secret DMT we investigate the perfect secrecy outage probability

$$\begin{aligned}
&P(\text{perfect secrecy outage}) && (13)\\
&= P\left(\sum_{j:\sigma_j \geq 1} \log \sigma_j^2 + \log \left| \mathbf{I}_n + \frac{m\mathrm{SNR}}{p} \mathbf{H}_D \mathbf{H}_E^{\perp} \mathbf{H}_D^{\dagger} \right| + o(1) < r_s \log \mathrm{SNR} \right) && (14)\\
&\doteq P\left(\log \left| \mathbf{I}_n + \frac{m\mathrm{SNR}}{p} \mathbf{H}_D \mathbf{H}_E^{\perp} \mathbf{H}_D^{\dagger} \right| < r_s \log \mathrm{SNR} \right) && (15)\\
&= \int ... \int P\left(\log \left| \mathbf{I}_n + \frac{m\mathrm{SNR}}{p} \mathbf{H}_D \mathbf{H}_E^{\perp} \mathbf{H}_D^{\dagger} \right| < r_s \log \mathrm{SNR} | \mathbf{H}_E^{(11)} = H_E^{(11)}, ..., \mathbf{H}_E^{(km)} = H_E^{(km)} \right) \\
&\qquad \cdot \prod_{i=1}^{k} \prod_{j=1}^{m} f_{\mathbf{H}_E^{(ij)}}(H_E^{(ij)}) dH_E^{(ij)} && (16)
\end{aligned}$$

For a fixed $\mathbf{H}_E = \mathrm{H}_E$, i.e. when all $\mathbf{H}_E^{(ij)} = H_E^{(ij)}$, $i = 1, ..., k$,$j = 1, ..., m$, the projection matrix $\mathrm{H}_E^{\perp}$ can be written as $\mathrm{H}_E^{\perp} = \mathrm{A}\mathrm{A}^{\dagger}$. The matrix A is of size $m \times (m-k)$. We can write $\mathrm{A} = [a_1, ..., a_{m-k}]$, where the length-$m$ column vectors a_j form an orthonormal basis for $\mathrm{Null}(\mathbf{H}_E)$. Let $\mathbf{H}_D = [\mathbf{r}_1^{\dagger}, ..., \mathbf{r}_n^{\dagger}]^{\dagger}$ be written in terms of length-m row vectors $\mathbf{r}_i$, $i = 1, ..., n$. Then each entry of $(\mathbf{H}_D \mathrm{A})^{(ij)} = \langle \mathbf{r}_i, a_j \rangle$, $i = 1, ..., n$, $j = 1, ..., (m-k)$. The mean value of each entry is equal to $E\{\langle \mathbf{r}_i, a_j \rangle\} = 0$. We observe that the covariance $E\{\langle a_j^{\dagger}, \mathbf{r}_i^{\dagger} \rangle \langle \mathbf{r}_s, a_t \rangle\} = a_j^{\dagger} E\{\mathbf{r}_i^{\dagger} \mathbf{r}_s\} a_t$. The value $E\{\mathbf{r}_i^{\dagger} \mathbf{r}_s\} = 1$, if $i = s$, and it is zero if $i \neq s$. In addition to these, as the vectors are orthonormal, $a_j^{\dagger} E\{\mathbf{r}_i^{\dagger} \mathbf{r}_s\} a_t = 0$, if $j \neq t$ for any i and s. Therefore, if $i = s$ and $j = t$, then $E\{\langle a_j^{\dagger}, \mathbf{r}_i^{\dagger} \rangle \langle \mathbf{r}_s, a_t \rangle\} = 1$; otherwise, it is equal to zero. Thus, $\mathbf{H}_D \mathrm{A}$ is a matrix, whose entries are i.i.d. Gaussian with zero mean and unit variance. Then we can write the probability in (16) as

$$\begin{aligned}
&P\left(\log \left| \mathbf{I}_n + \frac{m\mathrm{SNR}}{p} \mathbf{H}_D \mathbf{H}_E^{\perp} \mathbf{H}_D^{\dagger} \right| < r_s \log \mathrm{SNR} | \mathbf{H}_E^{(11)} = H_E^{(11)}, ..., \mathbf{H}_E^{(km)} = H_E^{(km)} \right) \\
&\qquad = P\left(\log \left| \mathbf{I}_n + \frac{m\mathrm{SNR}}{p} \mathbf{H}_D \mathrm{A}\mathrm{A}^{\dagger} \mathbf{H}_D^{\dagger} \right| < r_s \log \mathrm{SNR} \right) \\
&\qquad \doteq \mathrm{SNR}^{-d_{(m-k),n}(r_s)}.
\end{aligned}$$

In other words, this system is equivalent to an $(m-k) \times n$ MIMO with a well known DMT $d_{(m-k),n}(r_s)$

[14]. Substituting this value in (16), we observe that

$$\begin{aligned} P(\text{perfect secrecy outage}) &\doteq \int \ldots \int \frac{1}{\mathrm{SNR}^{d_{(m-k),n}(r_s)}} \prod_{i=1}^{k} \prod_{j=1}^{m} f_{\mathbf{H}_E^{(ij)}}(H_E^{(ij)}) dH_E^{(ij)} \\ &= \mathrm{SNR}^{-d_{(m-k),n}(r_s)}. \end{aligned}$$

To attain perfect secrecy the source uses i.i.d. complex Gaussian codewords with covariance matrix Q and transmits at rate $R^{(T)} = R_s^{(T)} + \log \left| \mathbf{I}_k + \mathbf{H}_E Q \mathbf{H}_E^\dagger \right|$ bits/channel use, where Q is the covariance matrix that attains the maximum in (11). Here the target secret communication rate is $R_s^{(T)}$ bits/channel use. Unlike the no CSIT case, the number of dummy codewords used for each secret message is variable and equal to $B = 2^{N \log \left| \mathbf{I}_k + \mathbf{H}_E Q \mathbf{H}_E^\dagger \right|}$. Then the main channel outage probability is equal to

$$\begin{aligned} P(\text{main channel outage}) &= P\left(\log \left| \mathbf{I}_n + \mathbf{H}_D Q \mathbf{H}_D^\dagger \right| < R^{(T)} \right) \\ &= P\left(\log \left| \mathbf{I}_n + \mathbf{H}_D Q \mathbf{H}_D^\dagger \right| - \log \left| \mathbf{I}_k + \mathbf{H}_E Q \mathbf{H}_E^\dagger \right| < r_s \log \mathrm{SNR} \right) \\ &= P(\text{perfect secrecy outage}) \\ &\doteq \mathrm{SNR}^{-d_{m-k,n}(r_s)}. \end{aligned}$$

Combining the upper and lower bounds (4) and (5) we conclude that the secret DMT is equal to $d_{m-k,n}(r_s)$ if $k < m$.

For the second case $n \leq k < m$, $p = 0$ by Lemma 1 and the high SNR secrecy capacity expression of [9] cannot be used directly. However, the converse and achievability in [9] can be extended to cover for $p = 0$, by deleting certain rows and columns in the generalized singular value decomposition [20]. Then the same secrecy capacity expression as in (12) holds with p replaced by $p' = \min\{m-k, n\}$. We can follow the same steps in the previous case to calculate $P(\text{perfect secrecy outage})$, and $P(\text{main channel outage})$ and find the secret DMT to be $d_{(m-k),n}(r_s)$ for $n \leq k < m$.

Finally for the last case, $k \geq m$, the secrecy capacity at high SNR is given by [19], [9]

$$\lim_{\mathrm{SNR} \to \infty} \tilde{C}_s(\mathrm{SNR}) = \sum_{j:\sigma_j \geq 1} \log \sigma_j^2. \tag{17}$$

As the capacity expression does not grow with increasing SNR, it is easy to see that the secret DMT is a single point $(0, 0)$. ■

In Fig. 1 secret DMT with CSIT is shown for $m = 3$, $n = 4$ and $k = 2$ in comparison to the secret DMT without CSIT and the DMT without secrecy constraints. The DMT without secrecy constraints, the

secret DMT with CSIT and the secret DMT without CSIT are shown to be respectively equal to $d_{3,4}(r)$, $d_{1,4}(r_s)$, and $d_{1,2}(r_s)$. In this example secrecy constraints impose both multiplexing gain and diversity gain losses whether CSIT exists or not.

On the other hand, if CSIT is available, secrecy constraints do not always result in multiplexing gain loss with respect to the DMT without secrecy constraints. This is illustrated in Fig. 2 for which the source, the destination and the eavesdropper respectively have 4, 2 and 1 antennas each. In this case, the secret DMT with full CSIT is equal to $d_{3,2}(r_s)$, $r_s \in [0, 2]$, whereas the secret DMT with no CSIT is equal to $d_{3,1}(r_s)$, $r_s \in [0, 1]$. Note that the secret DMT with no CSIT always experiences a degrees of freedom loss, whereas secret DMT with full CSIT only experiences secret diversity gain loss but not secret multiplexing gain loss, if $m - k \geq n$.

In Fig. 3 we compare the secret DMT for the wire-tap channel with a 2-antenna source, a 2-antenna destination, and a single antenna eavesdropper for no transmitter CSI and full CSI cases, as well as the DMT without secrecy constraints. The DMT without secrecy constraints is known to be $d_{2,2}(r)$, and according to Theorems 1 and 2, the secret DMT with no transmitter CSI and full CSI are equal to $1 - r_s$ and $2(1 - r_s)$ respectively. In Fig. 4 we compare secrecy outage probability for the same antenna numbers $m = 2$, $n = 2$ and $k = 1$. The secret multiplexing gain is assumed to be equal to 0.75; thus the secret diversity levels are equal to 0.25, if there is no CSIT, and 0.5 if CSIT is available. Fig. 4 confirms these results, from which we can observe the secret diversity to be approximately equal to the predicted values.

B. Alternative Achievability Schemes

In this section we propose a new secret DMT optimal scheme as an alternative to the capacity achieving strategy studied in Theorem 2, and compare it to the artificial noise scheme of [21].

1) Zero-forcing: Here we suggest a simple *zero-forcing* method that achieves the full CSIT secret DMT. As $k \geq m$ results in a trivial secret DMT, we assume $k < m$; i.e. $\mathbf{H}_E$ is not full column rank. In the zero-forcing protocol we transmit the secret information in $\mathbf{U}$, which is a length-$(m - k)$ column vector, and send $\mathbf{X} = \mathbf{A}\mathbf{U}$ at the transmitter, where $\mathbf{H}_E^{\perp} = \mathbf{A}\mathbf{A}^{\dagger}$. Then the received signals at the destination and the eavesdropper respectively become

$$\begin{aligned} \mathbf{Y}_D &= \mathbf{H}_D\mathbf{A}\mathbf{U} + \mathbf{Z}_D, \\ \mathbf{Y}_E &= \mathbf{H}_E\mathbf{A}\mathbf{U} + \mathbf{Z}_E \\ &= \mathbf{Z}_E. \end{aligned}$$

Stated differently, the destination observes an equivalent channel of $\mathbf{H}_D\mathbf{A}$, whereas the eavesdropper only observes noise because the secret message is transmitted in its null space. As the receiver knows the transmit strategy, it is also informed about $\mathbf{A}$ and thus about the equivalent channel. Then for every realization of $\mathbf{A}$, the equivalent channel gain matrix still has i.i.d. complex Gaussian entries with zero mean and unit variance. Assuming the covariance matrix of $\mathbf{U}$ is $m\mathrm{SNR}\mathbf{I}_{m-k}/(m-k)$, the achievable perfect secrecy rate (11) becomes

$$I(\mathbf{X};\mathbf{Y}_D) = I(\mathbf{U};\mathbf{Y}_D) = \log\left|\mathbf{I}_n + \mathbf{H}_D\mathbf{H}_E^{\perp}\mathbf{H}_D^{\dagger}\frac{m}{m-k}\mathrm{SNR}\right|$$

as $I(\mathbf{X};\mathbf{Y}_E) = 0$. For this equivalent channel the DMT can easily be shown to be $d_{m-k,n}(r_s)$ as in (13)-(16).

Note that for MIMO channels the source node can do beamforming in the direction of the destination, if CSI is available at the transmitter. Whether a secrecy constraint exists or not, beamforming in the direction of the destination only adds coding gain to the achievable mutual information $I(\mathbf{X};\mathbf{Y}_D)$ or $\log\left|\mathbf{I}_n + \mathbf{H}_D Q \mathbf{H}_D^{\dagger}\right|$ term in (11) and does not change the DMT [14] or the secret DMT. However, when there are secrecy constraints, the transmitter CSI can be used to control the *beam direction* of the message. With this information, when the message is transmitted in the null space of the eavesdropper, the secret DMT changes significantly as illustrated in the zero-forcing protocol.

2) Artificial Noise: In [21] the authors suggest an artificial noise scheme to increase achievable secrecy rates. In the artificial noise scheme the source node sends its messages in the range space of $\mathbf{H}_D$ and sends extra noise in $\mathbf{H}_D$'s null space. Let $\mathbf{T}$ be an $m \times (m-n)$ matrix, whose columns form an orthonormal basis for $\mathrm{Null}\mathbf{H}_D$, $\mathbf{V}$ is a length-$(m-n)$ column vector with i.i.d. complex Gaussian entries with zero mean, and $\mathbf{S}$ be a length-m column vector that carries source messages. Then source sends

$$\mathbf{X} = \mathbf{S} + \mathbf{T}\mathbf{V}.$$

As $\mathbf{V}$ is received in the null space of $\mathbf{H}_D$, the destination is not affected from this extra noise $\mathbf{V}$, but the eavesdropper is. Then the received signals at the destination and the eavesdropper are

$$\begin{aligned}\mathbf{Y}_D &= \mathbf{H}_D\mathbf{S} + \mathbf{Z}_D \\ \mathbf{Y}_E &= \mathbf{H}_E\mathbf{S} + \mathbf{H}_E\mathbf{T}\mathbf{V} + \mathbf{Z}_E.\end{aligned}$$

Assuming the covariance matrix for $\mathbf{S}$ and $\mathbf{V}$ are respectively $\mathrm{SNR}\mathbf{I}_m/2$ and $m\mathrm{SNR}\mathbf{I}_{m-n}/[2(m-n)]$, the achievable perfect secrecy (3) becomes equal to

$$R_s = \log\left|\mathbf{I}_n + \frac{\mathrm{SNR}}{2}\mathbf{H}_D\mathbf{H}_D^\dagger\right| - \log\frac{\left|\mathbf{K} + \frac{\mathrm{SNR}}{2}\mathbf{H}_E\mathbf{H}_E^\dagger\right|}{|\mathbf{K}|},$$

where $\mathbf{K} = \mathbf{I}_k + \frac{\mathrm{SNR}}{2(m-n)}\mathbf{H}_E\mathbf{T}\mathbf{T}^\dagger\mathbf{H}_E^\dagger$.

Simulations suggest that the artificial noise scheme also achieves the secret DMT $d_{(m-k),n}(r_s)$. A comparison between zero-forcing and artificial noise protocols is shown in Fig. 5 when the source has 2 antennas and the destination and the eavesdropper respectively have a single antenna each. The figure confirms that both schemes achieve a secret diversity 0.25, when the secret multiplexing gain is 0.75.

As a final note, the artificial noise scheme only necessitates the eavesdropper's instantaneous mutual information, $I(\mathbf{X};\mathbf{Y}_E)$, to determine the codebook structure; i.e. the sizes of the secret message set and the dummy codeword set. However, it does not necessitate the instantaneous channel gain matrix, $\mathbf{H}_E$. To do zero-forcing the instantaneous channel gain matrix is required but its outage probability performance is superior to artificial noise. In zero-forcing the source concentrates its power in the null space of $\mathbf{H}_E$ and it is guaranteed that the eavesdropper does not get any information. Thus, an advantage of zero forcing is that the source does not have to employ a secret codebook and send dummy information.

V. Conclusion

In this paper we study the MIMO wire-tap channel when there are stringent delay constraints and short-term power constraint. We define and find the *secret* DMT for arbitrary number of antennas at the source, the destination and the eavesdropper. First, we study no CSIT case. Our results show that the eavesdropper decreases the degrees of freedom in the direct link, $\min\{m,n\}$, by the degrees of freedom in the source-eavesdropper channel, $\min\{m,k\}$. The secret DMT depends on the remaining degrees of freedom. Therefore, if $k \geq m$, then no degrees of freedom is left for secure communication. Otherwise, the secret DMT is equivalent to that of a $(m-k)\times(n-k)$ MIMO without secrecy constraints. Then we study the effect of transmitter CSI on secret DMT. We observe that unlike the DMT without secrecy constraints, the transmitter CSI changes the secret DMT and it becomes equivalent to the DMT of a $(m-k)\times n$ MIMO if $k < m$; otherwise no tradeoff exists between secret multiplexing and secret diversity. We also suggest a zero-forcing scheme, which achieves the secret DMT bound when CSIT is available, and compare it to the artificial noise scheme.

APPENDIX I
PERFECT SECRECY OUTAGE PROBABILITY, NO CSIT

In Theorem 1 we need the probability of perfect secrecy rate outage. In this appendix, we first compute this probability for $k < \min\{m, n\}$. We will discuss the case $k \geq \min\{m, n\}$ at the end of the proof.

Secrecy Outage Lower Bound: Define $\mathcal{E}_l = \{\mu_i > a, i = 1, ..., k\}$, where a is a positive real constant and $\mathcal{E}_l^c$ denotes the complement of $\mathcal{E}_l$. Without loss of generality $a > 1$. Then we can write probability of secrecy rate outage as

$$\begin{aligned} &P(\text{perfect secrecy outage}) \\ &\quad = P(\text{perfect secrecy outage}|\mathcal{E}_l)P(\mathcal{E}_l) + P(\text{perfect secrecy outage}|\mathcal{E}_l^c)P(\mathcal{E}_l^c) \quad (18) \\ &\quad \geq P(\text{perfect secrecy outage}|\mathcal{E}_l)P(\mathcal{E}_l). \quad (19) \end{aligned}$$

As a is a constant, we find $P(\mathcal{E}_l)$ is also equal to a constant. At high SNR

$$\begin{aligned} &P(\text{perfect secrecy outage}|\mathcal{E}_l) \\ &\quad = P\left(\frac{\prod_{i=1}^{L}(1+\lambda_i \mathrm{SNR})}{\prod_{i=1}^{k}(1+\mu_i \mathrm{SNR})} < \mathrm{SNR}^{r_s}|\mathcal{E}_l\right) \quad (20) \\ &\quad \overset{(a)}{\geq} P\left(\frac{\prod_{i=1}^{L}(1+\lambda_i \mathrm{SNR})}{(1+a\mathrm{SNR})^{k}} < \mathrm{SNR}^{r_s}\right) \\ &\quad \overset{(b)}{\geq} P\left(\prod_{i=1}^{L}(1+\lambda_i \mathrm{SNR}) < \mathrm{SNR}^{r_s+k}\right) \\ &\quad \overset{(c)}{\doteq} \mathrm{SNR}^{-d_{m,n}(r_s+k)} \\ &\quad \overset{(d)}{\doteq} \mathrm{SNR}^{-d_{m-k,n-k}(r_s)}, \end{aligned}$$

where using the definition of $\mathcal{E}_l$ we substituted the minimum value for all μ_i in (20) to obtain (a). (b) follows because $(1+a\mathrm{SNR})^k \geq \mathrm{SNR}^k$. Using the DMT results without secrecy constraints [14], (c) and (d) follow. As $P(\text{perfect secrecy outage}) \doteq \mathrm{SNR}^{-d_s(r_s)}$, we conclude that $d_s(r_s)$ is upper bounded with the DMT of an $(m-k) \times (n-k)$ MIMO system.

Secrecy Outage Upper Bound: To make the upper bound tight, we need a piecewise analysis, which depends on the secret multiplexing gain. We define c_i as

$$c_i = -(m+n-2k-2i-1)r_s + (m-k)(n-k) - i(i+1),$$

for $i = 0, 1, ..., \min\{m, n\} - k - 1$. We also define the event $\mathcal{E}_{u,i} = \{\mu_k > c_i \log \mathrm{SNR}\}$, and $\mathcal{E}_{u,i}^c$ as the complement of $\mathcal{E}_{u,i}$.

For any i, we can write

$$\begin{aligned} & P(\text{perfect secrecy outage}) \\ &= P(\text{perfect secrecy outage}|\mathcal{E}_{u,i})P(\mathcal{E}_{u,i}) + P(\text{perfect secrecy outage}|\mathcal{E}_{u,i}^c)P(\mathcal{E}_{u,i}^c) \\ &\leq P(\mathcal{E}_{u,i}) + P(\text{perfect secrecy outage}|\mathcal{E}_{u,i}^c), \end{aligned} \tag{21}$$

where we have upper bounded both $P(\text{perfect secrecy outage}|\mathcal{E}_{u,i})$ and $P(\mathcal{E}_{u,i}^c)$ with 1.

To calculate an upper bound on the first term in (21), we use an upper bound on the probability density function (pdf) of μ_k. We obtain this bound using the joint pdf of the ordered eigenvalues $0 \leq \mu_1 \leq \mu_2 \leq ... \leq \mu_k$ of the matrix $\mathbf{H}_E\mathbf{H}_E^\dagger$ [14, Lemma 3], which is

$$p(\mu_1, ...\mu_k) = K_{m,k}^{-1} \prod_{i=1}^{k} \mu_i^{m-k} \prod_{i<j} (\mu_i - \mu_j)^2 e^{-\sum_{i=1}^{k} \mu_i},$$

where $K_{m,n}$ is a normalizing constant. Then,

$$\begin{aligned} & p(\mu_k) \\ &= \int_0^{\mu_k} ... \int_0^{\mu_2} p(\mu_1, ...\mu_k) d\mu_1 ... d\mu_{k-1} \\ &= K_{m,k}^{-1} \mu_k^{m-k} e^{-\mu_k} \\ &\quad \cdot \int_0^{\mu_k} ... \int_0^{\mu_2} \prod_{i=1}^{k-1} \mu_i^{m-k} \prod_{i<j} (\mu_i - \mu_j)^2 e^{-\sum_{i=1}^{k-1} \mu_i} \\ &\qquad\qquad d\mu_1 ... d\mu_{k-1} \\ &\overset{(e)}{\leq} K_{m,k}^{-1} \mu_k^{m-k} \mu_k^{k(k-1)} e^{-\mu_k} \\ &\quad \cdot \int_0^{\mu_k} ... \int_0^{\mu_2} \prod_{i=1}^{k-1} \mu_i^{m-k} e^{-\sum_{i=1}^{k-1} \mu_i} d\mu_1 ... d\mu_{k-1} \end{aligned} \tag{22}$$

$$\overset{(f)}{\leq} K_{m,k}^{-1} \mu_k^{m-k} \mu_k^{k(k-1)} e^{-\mu_k} [(m-k)!]^{k-1} \tag{23}$$

where (e) is because each $(\mu_i - \mu_j)^2 \leq \mu_k^2$, and there are $k(k-1)/2$ many $(\mu_i - \mu_j)^2$ terms involved.

Before we write (f) we first bound the innermost integral in (22) as

$$\begin{aligned}
&\int_0^{\mu_2} \mu_1^{m-k} e^{-\mu_1} d\mu_1 \\
&= \gamma(m-k+1, \mu_2) \\
&\overset{(g)}{=} (m-k)! \left[1 - e^{-\mu_2} \left(\sum_{l=0}^{m-k} \frac{\mu_2^l}{l!}\right)\right] \\
&\leq (m-k)!,
\end{aligned}$$

where $\gamma(.,.)$ is the lower incomplete gamma function. Note that for (g) we used the series expansion of this function [22]. Applying this result repeatedly to all the integrals in (22) leads to (f). Using this upper bound on the pdf of the largest eigenvalue μ_k, we can now find an upper bound on $P(\mathcal{E}_{u,i})$. Let $C_i = c_i \log \mathrm{SNR}$ for short hand notation. Then,

$$\begin{aligned}
&P(\mathcal{E}_{u,i}) \\
&= P(\mu_k > C_i) \\
&= \int_{C_i}^{\infty} p(\mu_k) d\mu_k \\
&\overset{(h)}{\leq} K_{m,k}^{-1} [(m-k)!]^{k-1} \int_{C_i}^{\infty} \mu_k^{m-2k+k^2} e^{-\mu_k} d\mu_k \\
&= K_{m,k}^{-1} [(m-k)!]^{k-1} \Gamma(m-2k+k^2+1, C_i) \qquad (24) \\
&\overset{(i)}{=} K_{m,k}^{-1} [(m-k)!]^{k-1} e^{-C_i} \sum_{l=0}^{m-2k+k^2} \frac{C_i^l}{l!}, \qquad (25)
\end{aligned}$$

where we used (23) to obtain (h). In (24) $\Gamma(.,.)$ denotes the upper incomplete Gamma function, and we used the series expansion of this function to obtain (i) [22]. Then, it is easy to show that

$$P(\mathcal{E}_{u,i}) \ \dot{\leq} \ \mathrm{SNR}^{-c_i}, \qquad (26)$$

as the e^{-C_i} term in (25) determines the high SNR behavior of (25).

For the second term in (21) we show that

$$\begin{aligned}
&P(\text{perfect secrecy outage}|\mathcal{E}_{u,i}^c)\\
&= P\left(\frac{\prod_{i=1}^{L}(1+\lambda_i\mathrm{SNR})}{\prod_{i=1}^{k}(1+\mu_i\mathrm{SNR})} < \mathrm{SNR}^{r_s}|\mathcal{E}_{u,i}^c\right)\\
&\overset{(j)}{\leq} P\left(\frac{\prod_{i=1}^{L}(1+\lambda_i\mathrm{SNR})}{(1+(c_i\log\mathrm{SNR})\mathrm{SNR})^k} < \mathrm{SNR}^{r_s}\right)\\
&\overset{(k)}{\leq} P\Bigg(\prod_{i=1}^{L}(1+\lambda_i\mathrm{SNR})\\
&\qquad < (2\max\{1,c_i\})^k(\log\mathrm{SNR})^k\mathrm{SNR}^{r_s+k}\Bigg)
\end{aligned}$$

$$\begin{aligned}
&\overset{(l)}{\leq} P\left(\prod_{i=1}^{L}(1+\lambda_i\mathrm{SNR}) < A^k(\log\mathrm{SNR})^k\mathrm{SNR}^{r_s+k}\right)\\
&\overset{(m)}{\doteq} \mathrm{SNR}^{-d_{m,n}(r_s+k)}\\
&\doteq \mathrm{SNR}^{-d_{(m-k),(n-k)}(r_s)}. \qquad (27)
\end{aligned}$$

In the above inequalities, (j) is because the largest eigenvalue μ_k and hence all μ_i's are upper bounded by $c_i\log\mathrm{SNR}$ given $\mathcal{E}_{u,i}^c$. (k) is due to the fact that

$$1+(c_i\log\mathrm{SNR})\mathrm{SNR} \leq 2\max\{1,c_i\}(\log\mathrm{SNR})\mathrm{SNR},$$

and (l) follows because $c_i \leq (m-k)(n-k)$, for all $i=1,...,\min\{m,n\}-k-1$, and we define $A=2\max\{1,(m-k)(n-k)\}$. Finally, (m) is because $A^k(\log\mathrm{SNR})^k\mathrm{SNR}^{r_s+k}$ has the same multiplexing gain as SNR^{r_s+k}, and thus the results in [14] apply.

Overall, substituting (26) and (27) into (21), using the definition of c_i, and combining the results for all i we have

$$P(\text{perfect secrecy outage}) \;\dot{\leq}\; \mathrm{SNR}^{-d_{(m-k),(n-k)}(r_s)}.$$

We can observe that this upper bound on probability of secrecy rate outage is the same as the lower bound we calculated above. We conclude that $P(\text{perfect secrecy outage})\doteq\mathrm{SNR}^{-d_s(r_s)} = \mathrm{SNR}^{-d_{(m-k),(n-k)}(r_s)}$ and the secret multiplexing gain satisfies $r_s \leq \min\{m,n\}-k$ for $k<\min\{m,n\}$.

If $k \geq \min\{m,n\}$, then $P(\text{perfect secrecy outage}|\mathcal{E}_l)$ in (19) takes a constant value and does not decay with SNR. As $P(\mathcal{E}_l)$ is also equal to a constant, $P(\text{perfect secrecy outage})$ is lower bounded by a fixed

value in $(0, 1]$. Thus, we conclude that when $k \geq \min\{m, n\}$, the secret DMT reduces to the single point $(0, 0)$.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, p. 1355, October 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, p. 339, May 1978.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, p. 451, July 1978.

[4] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy of capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, p. 4687, October 2008.

[5] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, p. 2470, June 2008.

[6] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proceedings of IEEE International Symposium on Information Theory*, 2005.

[7] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," September 2007, iEEE Transactions on Information Theory, to appear. [Online]. Available: http://arxiv.org/abs/0709.3541

[8] A. Khisti and G. W. Wornell, "The MIMOME channel," in *Proceedings of 45th Allerton Conference on Communication, Control and Computing*, October 2007. [Online]. Available: http://arxiv.org/abs/0710.1325

[9] ——, "Secure transmission with multiple antennas: The MIMOME wiretap channel," August 2008, submitted to IEEE Transactions on Information Theory. [Online]. Available: http://allegro.mit.edu/pubs/posted/journal/2008-khisti-wornell-it.pdf

[10] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel." [Online]. Available: http://arxiv.org/abs/0710.1920

[11] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proceedings of 41st Conference of Information Sciences and Systems*, Baltimore, MD, March 2007.

[12] R. Liu and H. V. Poor, "Multiple antenna secure broadcast over wireless networks," in *Proceedings of the First International Workshop on Information Theory for Sensor Networks*, June 18 - 20 2007.

[13] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proceedings of IEEE International Symposium on Information Theory*, 2006.

[14] L. Zheng and D. N. C. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels," *IEEE Transactions on Information Theory*, vol. 49, p. 1073, May 2003.

[15] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wire-tap channels," in *Proceedings of 45th Allerton Conference on Communication, Control and Computing*, September 2007.

[16] ——, "Compound wire-tap channels," December 2008, submitted to the EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security.

[17] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, August 2007.

[18] K. Khalil, M. Youssef, O. O. Koyluoglu, and H. E. Gamal, "On the delay limited secrecy capacity of fading channels," 2009, submitted to IEEE International Symposium on Information Theory.

[19] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proceedings of IEEE International Symposium on Information Theory*, June 2007.

[20] C. C. Paige and M. A. Saunders, "Towards a generalized singular value decomposition," *SIAM Journal on Numerical Analysis*, vol. 18, p. 398, June 1981.

[21] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, p. 2180, June 2008.

[22] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. Academic press, 2007.

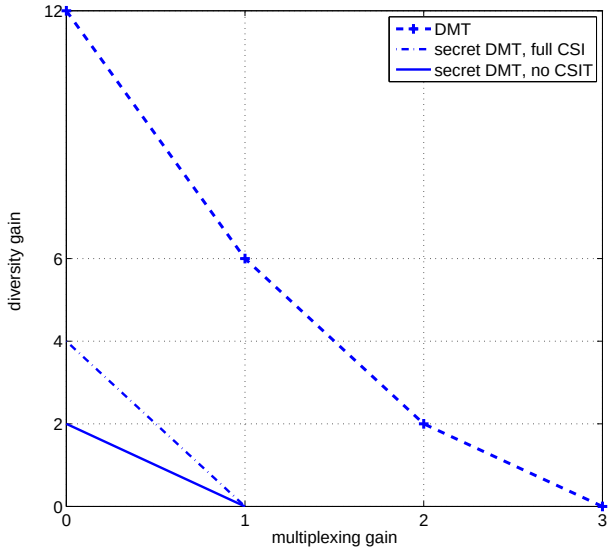

Fig. 1. The source, the destination and the eavesdropper respectively have 3, 4 and 2 antennas. The DMT with no secrecy constraints, secret DMT with transmitter and receiver CSI and, secret DMT with receiver CSI only are shown.

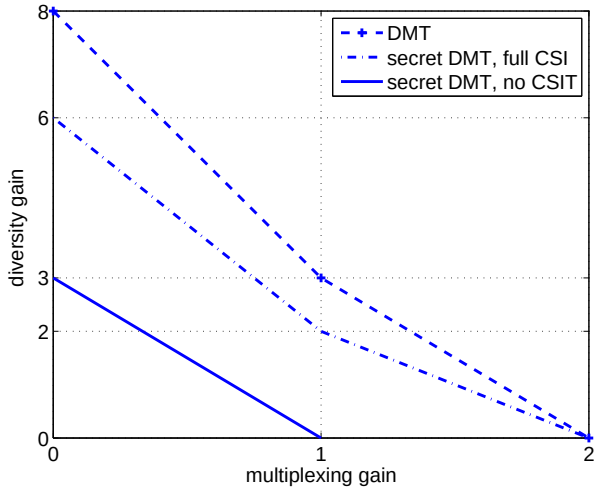

Fig. 2. The source, the destination and the eavesdropper respectively have 4, 2 and 1 antennas. The DMT with no secrecy constraints, secret DMT with transmitter and receiver CSI and, secret DMT with receiver CSI only are shown.

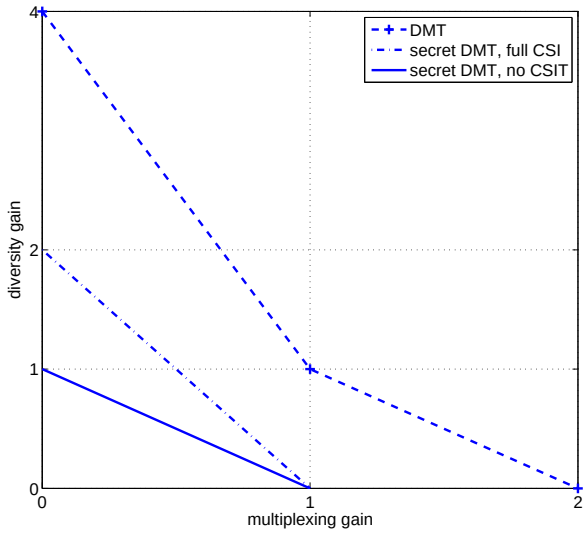

Fig. 3. The source, the destination and the eavesdropper respectively have 2, 2 and 1 antennas. The DMT with no secrecy constraints, secret DMT with transmitter and receiver CSI and, secret DMT with receiver CSI only are shown.

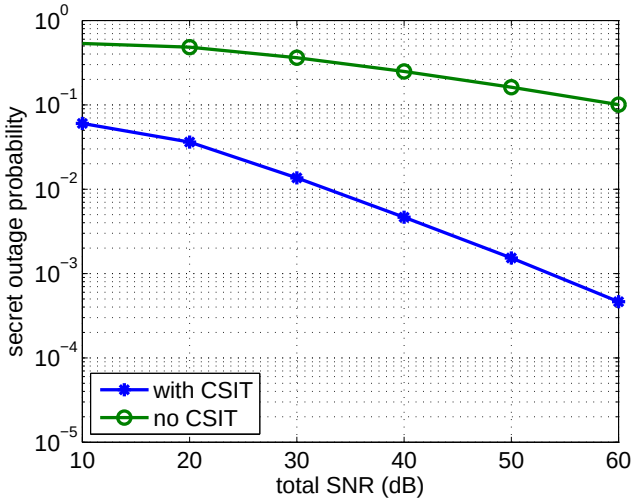

Fig. 4. The source, the destination and the eavesdropper respectively have 2, 2 and 1 antennas, $r_s = 0.75$.

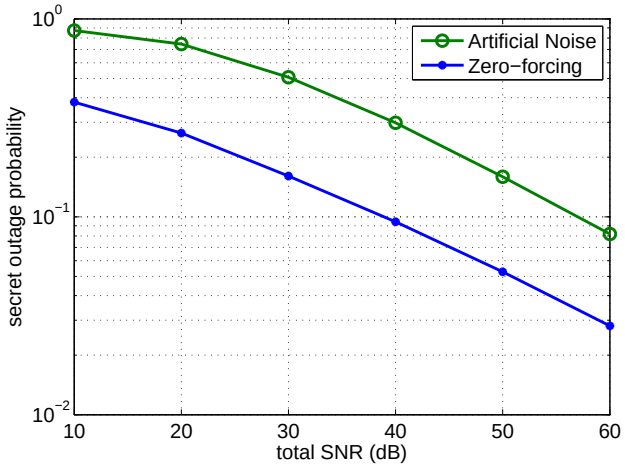

Fig. 5. The source has 2 antennas, and the destination and the eavesdropper each have a single antenna, $r_s = 0.75$.